科技论文全生命周期的安全问题与对策

王蕴[1]　吴炳潮[2] 关贝[2] 王永吉[2] —
1）国家税务总局税务干部学院（大连）
2）中国科学院软件研究所

摘　要：［目的］归纳与总结科技论文发表的全生命周期，探讨科技论文在全生命周期中的安全问题与解决措施，为加强保护科技论文中的涉密信息提供参考和借鉴；［方法］从科技论文全生命周期视角出发，分析在作者选题策划、作者单位审查、编辑部稿件处理、科技论文存档和科技论文流通五个阶段会存在的一些潜在安全性问题，针对问题给予建设性的意见与对策；［结果］为达到保证科技论文全生命周期安全性的目的，作者与需提高信息安全意识，作者单位划定安全保密的等级,编辑部培养兼顾专业性与保密安全意识的审稿人员，提高科技论文存储技术和数字水印技术；［结论］随着科技论文的网络化，随着而来的是信息泄露问题的增加，分析科技论文全生命周期的安全问题，并且探讨相应的对策，能有效地预防泄露科技领域中的敏感信息与情报。

关键词：　科技论文；科技论文全生命周期；科技论文安全对策
DOI：

互联网时代推动着科技革命的发展。知识信息、智慧价值、人才配置成为信息革命的创新源泉。在互联网时代，ACM、IEEE 等各种期刊与会议资源不断涌现，随之而来引发科技论文的发表数量集聚激增。随着互联网的普及，网络化成为科技论文最显著的新特点。自 2090 年代以来，随着互联网的飞速发展，人们的生活方式也发生了变化。广大科研人员充分利用自身优势，以最新的科技研究成果发表科技论文，实现了科技论文的网络化。科技论文网络化特征使信息无论在传播途径、传播效率，还是传播范围等方面都发生前所未有的大变革。随之也增加了信息泄密的概率与风险，例如阿里巴巴旗下“淘宝网”曾经遭遇过个人软件开发者使用自己设计的网页爬虫软件进行数据爬取，超过 11 亿条用户信息数据泄露。另外尤为关注的是，目前互联网学术期刊检索系统收录了自然科学和社会科学领域中绝大部分的科技论文，期刊检索平台在为科研工作者提供科技查证和科技查新数据库支持的同时，也存在着泄密风险。正如唐迪等[1]所指出的，海外情报机构利用期刊数据库开展情报收集活动，从公开发表的科技论文中获取我国科技领域的敏感信息和情报。因此，加强科技论文发表过程中的保密隐患刻不容缓。秦小雪等人[2]指出，科技期刊在互联网上的保密带来了挑战，一直是国外情报机构渗透和窃取信息的主要目标。中美贸易摩擦以来，技术竞争加剧，各种 “卡脖子” 技术受阻，如光刻机、工业软件等；

1 科技论文的全生命周期

全生命周期是一种交易理念和理论，全生命周期在不同的领域有着不同的阐释。科技论文的发表活动是一根完整的链条，这根链条构成科技论文发表的全生命周期。

1.1 全生命周期概念

全生命周期是一种交易理念和理论，在中心的实践探索中应运而生。在不同的领域，全生命周期有着不同的阐释。正如李满意等人[3]研究指出的，全生命周期管理思路、科技评审机制、保密评审机制。,软件的整个生命周期 (software life cycle，SLC) 是软件的生命周期，软件生命周期需求可行性分析，需求设计编码，调试和测试，验收和运营到放弃和智能制造企业的全生命周期是从产品设计数据到使用结束的生命周期，建立智能制造企业的产品生命周期管理平台，在产品和工艺设计、企业财务管理一体化等不同生命周期阶段的新型定制化生产模式创新，加速企业健康发展。

—通讯作者：王永吉[2] —

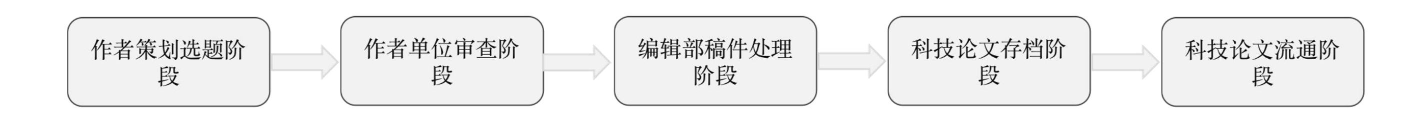


图 1 科技论文的全生命周期

1.2 科技论文的全生命周期

科技论文的发表活动是一根完整的链条，这根链条构成科技论文发表的全生命周期。科技论文的全生命周期包括作者选题策划、作者单位审查、编辑部稿件处理、科技论文存档和科技论文流通五个阶段，如图 1 所示。

第一阶段，作者策划选题阶段。作者在策划科技论文选题时，应当首先了解法律法规关于国家秘密范围和密级界定在科技论文相关领域划分的规定，最终确定选择科技论文选题的方向。第二阶段，作者单位审查阶段。科技论文会涉及科技生产的前沿领域，因此科技论文作者所属单位应当对科技成果进行审核，是否超出学术研究的范畴，做好科技成果及关键技术的密级划定，对创新成果的信息安全要做好保密审查工作。编辑部在论文的安全审查中起着至关重要的作用。编辑部的工作人员和审稿人要强化保密观念，通过严格的编辑制度，防止论文的保密信息泄露。编辑部的审查过程具体包括：草案任命、接收、初审和外部审查四个环节。正如高毅等人[4]提出的各种措施。第四阶段，科技论文存档阶段。随着互联网的发展，科技论文的信息存储载体模式从传统的纸质文献模式迅速向电子文献模式、电子文献、网络数据库、电子书刊等方向发展。这些数据存储介质传递信息迅速，对分类载体的管理薄弱，技术保护能力不足，失控风险较高。第五阶段，科技论文流通阶段。科技论文最终形成的科技成果将被纳入互联网学术期刊检索系统，广泛推广和交流。期刊检索网络平台科技学术文献学位论文等资源检索阅读下载服务，应防止科技论文被内部人员下载，私自传播给敌对势力，造成国内核心机密信息泄露。

2 科技论文全生命周期的安全问题

安全问题贯穿科技论文的全生命周期的五个阶段，根据科技论文全生命周期安全问题的特点，需要在科技论文全生命周期管理过程中提前识别风险，对潜在的信息安全风险进行分析。

2.1 作者选题策划阶段

在作者的选题策划阶段将存在的潜在信息安全问题包括作者对所研究的科学论文主题的保密知之甚少，以及作者在撰写科学论文时对机密信息的泄露。

(1) 作者对所研究的科技论文的保密性知之甚少。作者对自己所研究的科技论文课题的保密性知之甚少。在撰写科技论文之前，作者的保密意识淡薄，未按科技保密审查制度的规章制度执行科技论文课题中的保密性研判，而是按照自我认知进行科技论文保密性的判定；

(2) 作者在撰写科技论文时泄露保密信息。作者迫于职称晋升、学位答辩、业绩评定、绩效考核等压力，在撰写科技论文时，仅考虑科技论文投稿后的录用率，而过于详细描述了关键技术参数、技术方案、实现路径等涉及保密的科技成果。

2.2 作者单位审查阶段

科技论文在作者单位审查阶段会存在的潜在信息安全问题包括作者单位缺乏完善的定密工作以及作者单位的保密审查制度执行力不足。

(1) 作者单位缺乏完善的定密工作。合理的定密制度是决定科技论文审查有效性的关键步骤，做好科技论文定密工作，其基础任务是指定定密细目和细目的细化程度，从而保障国家安全和利益。

(2) 作者单位的保密审查制度执行力不足。《中华人民共和国保密法》第三条规定："一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。"科技论文作者单位虽然设立了保密评审机构，但大多缺乏兼具保密知识和科研生产业务的评审人员，导致科技论文保密评审制度流于形式，未能有效履行保密评审职责。

2.3 作者单位审查阶段

编辑部科技论文的稿件处理具体包括拟稿、接收、初审和外部评审四个分阶段。每个子阶段都会有潜在的信息安全问题。。在科技论文约稿阶段过程中，有的编辑部在征稿启事中会要求作者文责自负，提醒作者确保投稿的科技论文不涉及保密事项，但是却未按照规定设置保密条款，也未按照科技论文保密规定要求提供保密审查证明。在接收稿件的过程中，科学论文的稿件通过网络传输，可能受到间谍软件、木马和网络嗅探的攻击，导致机密信息泄露。在初审阶段过程中，期刊编辑人员数量和知识结构不合理，由于自身水平不足，无法察觉科技论文是否泄密。在外审阶段过程中，可能会混淆科技论文涉密内容和专业技术信息，发给外部专业审稿人，导致科技论文涉密信息泄露。

2.4 科技论文存档阶段

科技论文在网络数据库存放阶段会存在的潜在信息安全问题包括科技论文网络数据库遭遇病毒攻击以及网络数据库存在安全漏洞。

(1) 科技论文网络数据库遭遇病毒攻击。随着云计算、大数据等技术的发展，网络数据库在应用过程中不断遭受病毒的攻击。不法分子会通过植入木马病毒等方式破坏计算机网络的代码程序，干扰网络数据库的正常运行，窃取科技论文数据，导致科技论文的泄密。

(2) 科技论文网络数据库存在安全漏洞。互联网环境下，不存在完全安全的计算机网络数据库，网络黑客在网络数据库应用过程发现了程序漏洞，非法入侵科技论文网络数据库存储地址，窃取、修改网络数据库中的科技论文数据，造成科技论文网络数据库中的科研成果信息丢失或实验结果数据缺失，导致科技论文中的保密信息遭到泄露。

2.5 科技论文流通阶段

科技论文在流通过程中会存在的潜在安全性问题包括科技论文作者所属权益问题以及科技论文泄密追索问题。

(1) 科技论文作者所属权益问题。科技论文最终形成的科技成果将被纳入互联网学术期刊检索系统，广泛推广和交流。由于科技论文以文档形式呈现，现有的文档转换软件可以轻易提取科技论文的核心的数据信息，造成科技论文在流通阶段作者所属权益遭受侵害。

(2) 科技论文泄密追索问题。期刊检索网络平台学术文献科学学位论文等类型的资源检索与下载服务。科技论文应当在一定时间内限制公开、交流和使用范围，应当防止科技论文被内部人员下载，私自传播给敌对势力，导致国内核心机密信息被泄露。

3 科技论文全生命周期信息安全问题的对策

建立科技论文的全生命周期监控机制，实现对科技论文全生命周期的过程管理，有效防御和积极应对科技论文全生命周期五个阶段的信息安全问题。

3.1 作者选题策划阶段

(1) 加强自审，强化作者保密意识。科技论文作者应当定期参与单位组织的保密警示教育活动，强化科技论文保密意识，始终坚持涉密内容不发或经过脱密处理后再投稿的原则，从根源上杜绝科技论文泄密事件的发生。

(2) 在选题策划阶段，把握好回避原则。作者在进行科技论文相关方面选题时，应当回避国防科技发展和武器装备研究等涉密主题。撰写科技论文时，尽量减少应用涉密科研项目中的文件资料和图标，禁止将涉密成果直接发表。

3.2 作者单位审查阶段

(1) 完善审查定密工作，落实科技论文保密审查专人负责制。科技论文作者单位要在详细目的介绍的基础上，完善科技论文专职保密工作组织，规范科技论文评审流程。科技论文保密评审专员不仅需要掌握保密的法律法规和规章制度，还需要熟练掌握科技论文的专业技术。

(2) 加强科技论文保密知识教育。科技论文保密审查工作直接关系到国家安全和利益。科技论文作者单位应加强保密宣传工作，构筑保密防范的第一道“防火墙”。科技论文作者岗位特点，加强科技论文保密知识学习，增强科技成果保密意识，传播科技信息保密理念。

3.3 编辑部稿件处理阶段

(1) 在约稿阶段过程中，国家机密的论文或者涉及国防信息方面的内容是需要进行保密审查的，要求编辑部必须明确科技论文保密审查要求，明确保密内容撰写，积极落实保密制度的实施。

(2) 在接收稿件的过程中，可以通过密钥的方式提高科技论文网络数据库的安全性。正如卢建兰等研究[5]所指出的，密钥使网络数据库和科技论文访问者形成相应的契约关系。科技论文网络数据库可以采用实物、数字签名或生物特征数据密码的形式，为访问者提供相应的网络密码或密码，使数据在网络数据库和访问者之间实现点对点的安全信息传输，从而在接收阶段迅速完成注册验证过程，大大提高了科技论文的安全效果。

(3) 在初审阶段过程中，可采用两阶段人工审核和 AI 赋能审核，其中两阶段人工审核采用“初审 + 专家审模式”，在初审中筛选涉及保密的工作，后续由专家判定。通过 AI 赋能辅助审核，利用人工智能技术自动识别科技论文敏感信息或自动对科技论文敏感信息进行打码。

(4) 在外审阶段过程中，通过将科技论文审密和审稿分开，联系作者排除涉密内容后才交给外部审稿人，并且实行“外审专家认证制”，防止外审专家私自泄露科技论文的机密信息。

3.4 科技论文存档阶段

(1) 安装防火墙与安全软件。安装杀毒软件仅仅是防止电脑病毒的入侵科技论文网络数据库，而对于黑客的攻击就要借助于防火墙。防火墙作为一个阻断点，可以大大提高科技论文网络数据库的安全性，通过过滤不安全的服务，降低黑客窃取、破坏和篡改网络数据库中科技论文数据的网络风险，提高科技论文网络数据库安全防护能力。

(2) 采用数据库加密手段。数据加密是利用密钥加密等技术对信息提供保护的方法，其原理是利用密钥对科技论文加密，且只能利用相同的密钥对论文解密。通过对科技论文进行数据加密，黑客和非法侵入者只能看到呈现出乱码形式的科技论文数据。此外，还设置了安全密钥和访问认证机制。通过键的方法，使数据库和访问者形成相应的契约关系，使科技论文点对点地传输。

3.5 科技论文流通阶段

(1) 科学界定科技论文的数据产权。依据《中华人民共和国民法典》的规定，知识产权是权利人依法对作品、商标等客体享有的权利。数据信息一般不能作为知识产权客体，但科技论文中的数据产权属于知识产权保护的新领域。张俊宏等人[6]指出，”全国政协委员刘世锦今年在全国人大的提案中建议，要守住数据产权保护和数据安全的底线，应科学界定数据的初始产权和增值产权，平等保护数据流通不同环节各种产权的合理权益。”基于区块链技术的科技论文流通方法。石冠彬等[7]指出，区块链技术通过构建“司法联盟链”，可以确保其在各个阶段不被篡改或伪造，从而使其成为原始证据。用区块链技术构建底层可信联盟链网络，科技论文在资源检索、在线阅读和下载服务等阶段形成区块链交易信息进行申请和提

交，从而彻底解决科技论文作者的权益和科技论文泄密追索问题[8, 9]。

4 结语

综上所述，随着互联网的普及，科技论文网络化加大了信息泄密的概率与风险。完善科技论文全生命周期的监控制度，编辑部组织专家对科技论文全生命周期的信息安全进行检查和督导，需对检查和指导各个环节中的操作规范，并记录原始的科研数据；科技论文全生命周期中各环节的工作人员严格审核科技论文的保密信息，严格按照相关既定制度办事，编辑部安排监管人员定期检查工作。另外，研发科技论文全生命周期的监控工具，针对编辑部的工作人员的精力有限和专业知识有限等问题，通过人工智能赋能来研发监控工具，用于自动监控科技论文全生命周期中的不合规操作并根据规章制度给予相应的建议。

参考文献：

[1] 唐迪,夏雪莲.科技论文发表过程中存在的保密问题及对策[J].保密科学技术,2015(01): 62-64.

[2] 秦晓雪.科技期刊泄密风险及保密管理对策分析[J].出版与印刷,2021(02):67-71.

[3] 李满意.关于科技期刊稿件全生命周期保密审查机制的思考[J]. 编辑学报,2014(S1):12-13.

[4] 高毅,王艳秀,张桂弘,姜梅.浅谈如何做好科技期刊的保密工作[J].科技传播,2020,12(24):26-28.

[5] 芦建兰.计算机网络数据库安全问题研究[J].电子测试,2021(14):133-134.

[6] 张军红.全国政协委员刘世锦：平衡好数据安全与流通关系[J].经济,2022(04):36.

[7] 石冠彬,陈全真.论区块链存证电子数据的优势及司法审查路径[J].西南民族大学学报(人文社会科学版),2021(01):67-73.

[8] 赵精武.从保密到安全：数据销毁义务的理论逻辑与制度建构[J].交大法学,2022(02):28-41.

[9] 代妮.科技期刊应加强保密工作[J].编辑学报,2022,34(03):244-248.

Safety Problems and Countermeasures of Scientific Papers in the Whole Life Cycle

Abstract

[Purposes] Summarize and summarize the entire life cycle of scientific papers published, discuss the security problems and solutions in the entire life cycle of scientific papers, and provide reference and reference for strengthening the protection of classified information in scientific papers.

[Methods] From the perspective of the whole life cycle of scientific papers, this paper analyzes some potential security problems that will exist in the five stages of author topic selection planning, author unit review, editorial manuscript processing, scientific paper archiving and scientific paper circulation, and gives constructive suggestions for the problems. opinions and countermeasures;

[Findings] To achieve the purpose of ensuring the security of scientific papers in the whole life cycle, the authors need to improve their awareness of information security, and the author unit defines the level of security and confidentiality. digital watermarking technology;

[Conclusions] With the networkization of scientific papers and the increase of information leakage problems,

analyzing the security problems of the whole life cycle of scientific papers and discussing corresponding countermeasures can effectively prevent the leakage of sensitive information and intelligence in the field of science and technology.

Keyword: Scientific papers; Scientific papers in the whole life cycle; Safety and countermeasures of scientific papers.

[作者贡献声明]：
作者 1：组织论文架构，撰写论文；
作者 2：文献调研与整理；
作者 3：起草论文、修订论文、审核论文;
作者 4: 参与论文修订、论文最终版本修订.